III. REMARKS

Claims 1-6 and 8-31 are pending in the present application. Claims 7 and 32 were previously canceled. In this amendment, applicant has canceled claims 1-6, 8-16 and 24-31. Applicant is not conceding that the subject matter encompassed by claims 1-6, 8-16 and 24-31, prior to this Amendment is not patentable over the art cited by the Examiner. Claims 7 and 31 previously cancelled, and claims 1-6, 8-19, 27-30, and 32-35 canceled in this Amendment were canceled solely to facilitate expeditious prosecution of the remaining claims. Applicant respectfully reserves the right to pursue claims, including the subject matter encompassed by claims 1-16 and 24-32, as presented prior to this Amendment and additional claims in one or more continuing applications.

Claim Rejections - 35 U.S.C. § 101

The examiner has rejected claims 24-30 under 35 U.S.C. § 101 as being directed towards non-statutory subject matter. Claims 24-30 have been canceled as discussed above. Therefore, the rejection is moot.

Claim Rejections - 35 U.S.C. § 103, Obviousness

The examiner rejected claims 17-23 under 35 U.S.C. § 103 as being unpatentable over U.S. Patent Application Publication No. 2003/0041266 A1 to Ke et al., hereinafter Ke, in view of U.S. Patent No. 2002/0165949 A1 to Na et al., hereinafter Na. This rejection is respectfully traversed. Claims 17-23 remain pending.

Claim 17

Claim 17 recites "a method for analyzing a packet using a firewall which creates a plurality of trust levels for a plurality of computer networks." Applicant submits that Ke does not disclose a firewall that "creates a plurality of trust levels for a plurality of networks."

Claim 17 further recites "using a single router containing the firewall and a switch to service each of the plurality of computer networks." The examiner cites Ke, FIG. 2, block 210 and paragraphs 0033 and 0034. Ke's firewall 210 is a firewall device that is separate from the routers. Ke's firewall 210 does not contain "a switch to service each of the plurality of computer networks."

Claim 17 further recites "wherein a trust level is a security level associated with a particular set of rules in the firewall." The examiner cites Ke, paragraphs 0018, 0031, and 0033. Ke discloses a set of security domain policies." Ke does not disclose a "trust level" that is associated with a particular set of rules in the firewall.

Claim 17 further recites "wherein the trust level reduces the time required for the firewall to analyze and either permit or deny the packet." The examiner admits that Ke does not teach that the trust level reduces the time required for the firewall to analyze and either permit or deny the packet. The examiner states that Na teaches a plurality of security policies that are prioritized (paragraph 0023, 0054) and a system for minimizing the packet delay time while it traverses through the various polices (paragraphs 0002, 0018, 0021, 0024, and 0046). Further the examiner stated that it would have been obvious to reduce the residence time in the firewall, since Na states at paragraph 0002 and 0018 that reducing the residence time, or delay time as discussed by Na, at the firewall improves the overall performance. Applicant submits that Na

does not disclose the use of a trust level to reduce the packets residence time in the firewall because as defined above in claims 17 the trust level is a "security layer associated with a set of rules in the firewall." Na is silent regarding associating a trust level with a set of rules.

Claim 18

Claim 18 recites "the method of claim 17 further comprising: responsive to a determination that the rules do not permit or deny the packet, denying the packet." The examiner cites Ke, FIG. 5, block 530 and paragraph 0051. Paragraph 0051 states that "[i]f no virtual system context can be found, the packet is dropped and the event is logged" and if a virtual system context has been found, "the packet will be subjected to firewall/VPN/traffic shaping processing in the same way as the packet would be processed on a stand-alone device." A virtual system context is not the same as the rules in applicant's claim.

Claim 19

Claim 19 recites the method of claim 17 wherein a table defines the relationship between the plurality of trust levels, the rules, and the computer networks." The examiner cites Ke, paragraph 0053, 0055, stating Ke discloses "policy-based and session-based lookup table, classification policies." Ke states that "[f]or non-tunnel traffic, a policy-based and session-based look-up table may be used to identify a virtual system context for the traffic from an untrusted interface." But this is not a table defining a relationship between trust levels, rules and computer networks.

Claim 20

Claim 20 recites "a method for analyzing a packet using a firewall which creates a plurality of trust levels for a plurality of computer networks." Applicant submits that Ke does not disclose a firewall that "creates a plurality of trust levels for a plurality of networks."

Claim 20 further recites "using a single router containing the firewall and a plurality of sub-switches to service each of the plurality of computer networks." The examiner cites Ke, FIG. 2, block 210 and paragraphs 0033 and 0034. Ke's firewall 210 is a firewall device that is separate from the routers in Ke. Ke's firewall 210 does not "contain" "a switch to service each of the plurality of computer networks."

Claim 20 further recites "determining a sub-switch location of a packet." The examiner cites Ke, paragraphs 0033-0034. Paragraphs 0033-0034 disclose determining "what VLAN the packet is intended for" but are silent as to "determining a sub-switch location of a packet." Ke is silent as to a router containing a firewall and sub-switches.

Claim 20 further recites "determining a source and a destination of the packet from a packet header." In regard to determining a source, the examiner cites Ke paragraphs 0047, and 0052 ("determining if the incoming packet is from a trusted or an untrusted interface." Applicant submits that determining whether an *interface* is trusted or untrusted is not the same as determining a *source*.

Claim 20 further recites "determining if the packet is attempting to go to a destination with a higher trust level than a trust level of the source" and "responsive to a determination that the packet is not attempting to go to a higher trust level, permitting the packet to pass to the destination." The examiner admits that Ke does not teach determining if the packet is attempting to go to a higher trust level" or permitting the packet if it is not attempting to go to a higher trust level. But the examiner states it would be obvious because Ke discloses at paragraph 0039, 0059-0122 a system for configuring the rules and policies of the firewall system." Ke is silent as to a comparison of a trust level of source and of a destination to make a determination.

Claim 20 further recites "wherein a trust level is a security level associated with a particular set of rules in the firewall." The examiner cites Ke, paragraphs 0018, 0031, and 0033. Ke discloses a set of security domain policies." Ke does not disclose a "trust level" that is associated with a particular set of rules in the firewall.

Claim 20 further recites "wherein the trust level reduces the time required for the firewall to analyze and either permit or deny a packet." The examiner admits that Ke does not teach that the trust level reduces the time required for the firewall to analyze and either permit or deny the packet. The examiner states that Na teaches a plurality of security policies that are prioritized (paragraph 0023, 0054) and a system for minimizing the packet delay time while it traverses through the various polices (paragraphs 0002, 0018, 0021, 0024, and 0046). Further the examiner stated that it would have been obvious to reduce the residence time in the firewall, since Na states at paragraph 0002 and 0018 that reducing the residence time, or delay time as discussed by Na, at the firewall improves the overall performance. Applicant submits that Na does not disclose the use of a trust level to reduce the packets residence time in the firewall because as defined above in claims 17 the trust level is a "security layer associated with a set of rules in the firewall." Na is silent regarding associating a trust level with a set of rules.

Claim 21

Claim 21 recites "the method of claim 20, wherein responsive to a determination that the packet is attempting to go to a higher trust level, the method further comprises: determining the appropriate rules to use to analyze the packet using the table; analyzing the packet using the rules; determining if the packet is permitted under the rules; responsive to a determination that the rules permit the packet, permitting the packet; and responsive to a determination that the rules deny the packet, denying the packet." The examiner cites Ke, FIG. 5, block 515, 520, 525,

530, 540, 0049-0050, and 0051. Paragraphs 00049-0051 discuss global traffic policies and a virtual system context which are different from the claim recitations. Paragraph 0051 states that "[i]f no virtual system context can be found, the packet is dropped and the event is logged" and if a virtual system context has been found, "the packet will be subjected to firewall/VPN/traffic shaping processing in the same way as the packet would be processed on a stand-alone device." A virtual system context is not the same as the rules in applicant's claim.

Claim 22

Claim 22 recites "the method of claim 21 wherein the security program further comprises: responsive to a determination that the rules do not permit or deny the packet, denying the packet." The examiner cites Ke, FIG. 5 block 530, 0051. Ke discloses dropping a packet if a virtual system context is not found. Ke does not disclose "a determination that the rules do not permit or deny the packet." Ke is silent as to "denying" a packet, and that such an action takes place after the determination discussed above.

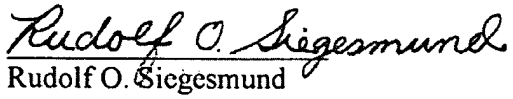
Claim 23

Claim 23 recites "the method of claim 20 wherein the firewall further comprises: a table defining the relationship between the trust levels, the rules, and the computer networks." The examiner cites Ke, paragraph 0053, 0055, stating Ke discloses "policy-based and session-based lookup table, classification policies." Ke states that "[for non-tunnel traffic, a policy-based and session-based look-up table may be used to identify a virtual system context for the traffic from an untrusted interface." But this is not a table defining a relationship between trust levels, rules and computer networks. In particular, the trust levels and the rules are those defined in applicants claim 17.

Conclusion

Applicant submits that the claims are now in condition for allowance.

Respectfully submitted,



Rudolf O. Siegesmund
Registration No. 37,720
Gordon & Rees LLP
Suite 2800
2100 Ross Avenue
Dallas, Texas 75201
214-231-4660
214-461-4053 (fax)
rsiegesmund@gordonrees.com